TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
12/29/2016

SUBJECT:
Multiple Vulnerabilities in Mozilla Thunderbird Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been identified in Mozilla Thunderbird, which could allow for arbitrary code execution. Mozilla Thunderbird is an email client. Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code in the context of the user running the affected application. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:

- Thunderbird prior to 45.6

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:

Mozilla has confirmed multiple vulnerabilities in Thunderbird. Exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution. These vulnerabilities could be exploited if a user visits or is redirected to a specially-crafted webpage or opens a specially-crafted file. Details of these vulnerabilities are as follows:

- A use-after-free vulnerability that occurs due to an error in the handling of node adoption. Specifically, this issue occurs when manipulating DOM events and removing audio elements. (CVE-2016-9899)
- A security bypass vulnerability that occurs because event handlers on marquee elements were executed despite a strict Content Security Policy (CSP) that disallowed inline JavaScript. (CVE-2016-9895)
- A memory-corruption vulnerability that occurs within the 'libGLES' development package. Specifically, this issue results in a potentially exploitable crash during 'WebGL' functions using a vector constructor with a varying array. (CVE-2016-9897)
- A use-after-free vulnerability that occurs when manipulating DOM subtrees in the Editor. An attacker can leverage this issue to crash the affected application. (CVE-2016-9898)
- A security bypass vulnerability that occurs because restricted external resources can be loaded by 'SVG' images through data URLs. An attacker can leverage this issue to cause cross-domain data leakage. (CVE-2016-9900)
- An information disclosure vulnerability that occurs because it allows to determine whether an atom is used by another compartment/zone in specific contexts. An attacker can leverage this issue to obtain usernames embedded in JavaScript code, across websites. (CVE-2016-9904)

- A potential exploitable crash in EnumerateSubDocuments exists. Specifically, this issues occurs when sub-documents get added or removed (CVE-2016-9905)
- A memory safety bugs present in Firefox 50.02 and Firefox ESR 45.5.1, which if exploited could lead to arbitrary code being run. (CVE-2016-9893)

Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code in the context of the user running the affected application. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate updates provided by Mozilla to vulnerable systems, immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Mozilla:
https://www.mozilla.org/en-US/security/advisories/mfsa2016-96/

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9899
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9895
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9897
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9898
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9900
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9904

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9905
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9893